We claim:

1. A cryptographic key split combiner that creates a cryptographic key to secure one or more respectively tagged data elements, comprising:

a plurality of key split generators for generating cryptographic key splits based on seed data; and

a key split binder for binding the cryptographic key splits together to produce the cryptographic key;

wherein at least one of the cryptographic key splits is based on at least one of the one or more respective tags.

2. The cryptographic key split combiner of claim 1, wherein the cryptographic key is one of a symmetric key and an asymmetric key.

3. The cryptographic key split combiner of claim 1, wherein the seed data for the at least one cryptographic key split is based on the at least one of the one or more respective tags.

4. The cryptographic key split combiner of claim 1, wherein the at least one of the one or more respective tags is the seed data for the at least one cryptographic key split.

5. The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a random split generator for generating a random split based on reference data.

6. The cryptographic key split combiner of claim 5, wherein said plurality of key split generators further includes a label split generator for generating a label split based on tag data.

7. The cryptographic key split combiner of claim 1, wherein said plurality of key split generators further includes a label split generator for generating a label split based on tag data.

8. The cryptographic key split combiner of claim 1, wherein the at least one of the one or more respective tags corresponds to at least one of a role, a rule and a privilege.

9. The cryptographic key split combiner of claim 1, wherein the at least one of the one or more respective tags corresponds to at least one label based on one of a role, a rule and a privilege.

10. A process of creating a cryptographic key to secure one or more respectively tagged data elements, comprising:

generating a plurality of cryptographic key splits from seed data; and

binding the cryptographic key splits together to produce the cryptographic key;

wherein at least one of the cryptographic key splits is based on at least one of the one or more respective tags.

11. A process of cryptographically securing one or more respectively tagged data elements, comprising:

generating a plurality of cryptographic key splits from seed data;

binding the cryptographic key splits together to produce a cryptographic key; and

encrypting the one or more respectively tagged data elements with the cryptographic key;

wherein at least one of the cryptographic key splits is based on at least one of the one or more respective tags.

12. A process of transporting keying data corresponding to a cryptographic key used to decipher one or more respectively tagged, cryptographically secured, data elements, comprising:

selecting the keying data corresponding to the cryptographic key; and

sending the selected keying data to an intended recipient.

13. The process of claim 12, wherein the keying data comprises data needed to create the cryptographic key by a recipient.

14. The process of claim 12, wherein the keying data comprises at least one of one or more key splits, one or more instances of seed data, one or more key identifiers and one or more algorithm identifiers.

15. The process of claim 12, wherein the keying data is encrypted before sending.

16. The process of claim 15, wherein the keying data is encrypted based on an encryption key, and the keying data comprises a key identifier corresponding to the encryption key.

17. The process of claim 15, wherein the keying data is encrypted based on an encryption key and an encryption algorithm, and the keying data comprises an encryption algorithm identifier corresponding to the encryption algorithm.

18. The process of claim 15, wherein the keying data is encrypted based on an encryption key and an encryption algorithm, and the keying data comprises an encryption key identifier and an encryption algorithm identifier corresponding to the encryption algorithm.

19. The process of claim 15, further comprising: formatting the keying data according to a cryptographic message syntax.

20. A method of providing multi-level cryptographic security of respectively tagged data elements, comprising:

accessing a constructive key manager;

selecting at least one respectively tagged data element from a data instance;

for each selected data element,

generating a cryptographic key based on the respective tag of the selected data element,

encrypting the selected data element based on the cryptographic key,

labeling the encrypted data element with the respective tag, and

storing the respectively tagged encrypted data element;

reading the respective tag of the at least one encrypted data element;

determining access authorization based on the respective tag; and

decrypting the data element if access authorization is granted.

21. The method of claim 20, further comprising:

for each selected data element, embedding the respectively tagged encrypted data element encrypted object in a second data element.